

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Krista Wittman on 9/30/2008.

The application has been amended as follows:

Claim 2. A system according to Claim 1, wherein the short range interface logically defines a secured area around the implantable medical device within which to securely obtain the crypto key and further wherein the long range interface logically defines a non-secured area extending beyond the secured area within which to exchange the encrypted [[data]] sensitive information.

Claim 3. A system according to Claim 1, wherein the encrypted [[data]] sensitive information is retrieved from the implantable medical device over a non-secure connection and the encrypted [[data]] sensitive information is decrypted as the sensitive data using the crypto key.

Claim 4. A system according to Claim 3, wherein the crypto key is securely retrieved over a secure connection from the secure key repository prior to decrypting the encrypted [[data]] sensitive information.

Claim 5. A system according to Claim 3, wherein the encrypted [[data]] sensitive information is retrieved through long range telemetry.

Claim 15. A method according to Claim 14, further comprising:
logically defining a secured area around the implantable medical device within which to securely obtain the crypto key; and
logically defining a non-secured area extending beyond the secured area within which to exchange the encrypted [[data]] sensitive information.

Claim 16. A method according to Claim 14, further comprising:
retrieving the encrypted [[data]] sensitive information from the implantable medical device over a non-secure connection; and
decrypting the encrypted data as the sensitive [[data]] information using the crypto key.

Claim 17. A method according to Claim 16, further comprising:
securely retrieving the crypto key over a secure connection from the secure key repository prior to decrypting the encrypted [[data]] sensitive information.

Claim 18. A method according to Claim 16, further comprising:
retrieving the encrypted [[data]] sensitive information through long range
telemetry.

Claim 28. An implantable medical device for securely maintaining sensitive
information, comprising:

- an implantable medical device, comprising:
 - a receiver to receive sensitive information via a long range interface and a copy
of at least a part of the sensitive information via a short range interface;
 - a memory to store the sensitive information encrypted using a crypto key
uniquely associated with an implantable medical device and to further store the copy as
unencrypted data; and
 - a secure interface to provide access to the stored sensitive information
exclusively over a secure connection.

Claim 29. An method for securely maintaining sensitive information on an
implantable medical device, comprising:

- receiving sensitive information via a long range interface and a copy of at least a
part of the sensitive information via a short range interface;

storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and further storing the copy as unencrypted data; and

providing access to the stored sensitive information exclusively over a secure connection.

Claim 30. An apparatus for securely maintaining sensitive information on an implantable medical device, comprising:

means for receiving sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface;

means for storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and means for further storing the copy as unencrypted data; and means for providing access to the stored sensitive information exclusively over a secure connection.

Allowable Subject Matter

1. Claims 1-6, 8-19, 21-30 are allowed.

The following is an examiner's statement of reasons for allowance: Applicant's arguments presented on pages 11-15 of the remarks submitted 5/12/2008 and supported by the specification at pages 11-16 are persuasive.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2434

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Examiner, Art Unit 2434

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434